DATA GOVERNANCE HANDBOOK

AUTAUGA COUNTY SCHOOLS

SPENCE AGEE, SUPERINTENDENT

EVERY STUDENT A GRADUATE; EVERY GRADUATE A SUCCESS

Autauga County Schools

Data Governance

The following documents are affiliated with Autauga County Schools Data Governance policy, procedures, training, and guidance.

Table of Contents

Introduction

Student and staff privacy is a necessary priority for all schools. The Autauga County School District is committed to maintaining strong and meaningful privacy and security protections. The privacy and security of all student and teacher information is a significant responsibility, as we value the trust of our students, parents, and staff.

The Autauga County Schools Data Governance Handbook includes information regarding the Data Governence committee, the Data Governance and Use Policy, security measures, and quality controls. The document formally outlines how operational and instructional activity shall be carried out to ensure that data is accurate, accessible, consistent, and protected. The document also establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

2014-2015 Data Governance Committtee

The Data Governance Policy and corresponding handbook were developed and implemented in the summer and fall of 2014. Committee members were responsible for researching assigned subsections and making recommendations. While the Data Governance Policy was adopted November, 2014, this compendium handbook is a living document. With the Board's permission, the Data Governance Committee can quickly modify information within the handbook in response to changing needs. All modifications will be posted on the Autauga County Schools website.

The Data Governance Committee is responsible for working with user management, owners, custodians, and users to develop and implement prudent policies procedures, and controls, subject to the approval of the school district. Specific responsibilities include:

1. Ensuring security policies, procedures, and standards are in place and adhered to by entity.
2. Providing basic security support for systems and users.
3. Advising owners in the identification and classification of computer resources.
4. Advising system development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
6. Providing ongoing employee security education.
7. Performing security audits.

The Autauga County School 2014-2015 Data Governance Committee is as follows:

Name	Department	Handbook Responsibility
Spence Agee	Superintendent	Data Governance Policy
Tisha Addison	Operations/Technology	Data Governance Policy
Rebecca Grigsby	Technology	Data Governance Policy
Rachel Surles	Assessment/Accountability	Data Manager
Alisa Benson	Finance	Banking Security
Angel Garrett	Pupil Services/Secondary Curriculum	Data Security Measures
Nancy Jackson	Personnel	Data Security Measures
Sandie Manscill	Health Services	Data Security Measures
Celeste Minor	Special Education	Email Use and Security Agreement
Audra Seagars	Child Nutrition	Data Backup and Retention
Tammy Starnes	Federal Programs/Elementary Curriculum	Student Information Systems & INOW Permissions
Janice Stockman	Principal	Student Information Systems & INOW Permissions
Raymond Thebo	Technology	Data Security Measures and Data Backup & Retention
Jodi Womble	Principal	Data Governance Training & Data Quality Controls

The Autauga County Schools administrative team, including principals and assistant principals, will serve in an advisory capacity to the committee and will be called upon to attend meetings as needed. The Data Governance Committee will meet a minimum of twice per year. Additional meetings will be called as needed.

Information Security Definitions and Responsibilites

Information Owner: The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner

may delegate ownership responsibilities to another individual by completing the District's Information Owner Delegation Form. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from the Legal Department.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the Data Governance Committee the loss or misuse of the District's information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the Data Governance Committee, where appropriate.
9. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

Custodian: The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
5. Evaluating the cost effectiveness of controls.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the Data Governance Committee.
7. Promoting employee education and awareness by utilizing programs approved by the Data Governance Committee, where appropriate.
8. Reporting promptly to the Data Governance Committee the loss or misuse of the District's information.
9. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

User Management: District supervisors who manage users as defined below. User management is responsible for overseeing their employees' use of information, including:

1. Reviewing and approving all requests for their employee's access authorizations.
2. Initiating security change requests to keep employees' security record current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the Data Governance Committee the loss or misuse of the District's information.
7. Initiating corrective actions when problems are identified.
8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

User: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.
2. Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.
3. Keep personal authentication devices (e.g. passwords, Secure Cards, PINs, etc.) confidential.
4. Report promptly to the Data Governance Committee the loss or misuse of the District's information.
5. Initiate corrective actions when problems are identified.

State Monitoring Checklist Cross-Reference

	ON-SITE	INDICATORS
1.	Has the data governance committee been established and roles and responsibilities at various levels specified?	Dated minutes of meetings and agendas Current list of roles and responsibilities
2.	Has the local school board adopted a data governance and use policy?	Copy of the adopted data governance and use policy Dated minutes of meetings and agenda
3.	Does the data governance policy address physical security?	Documented physical security measures
4.	Does the data governance policy address access controls and possible sanctions?	Current list of controls Employee policy with possible sanctions
5.	Does the data governance policy address data quality?	Procedures to ensure that data are accurate, complete, timely, and relevant
6.	Does the data governance policy address data exchange and reporting?	Policies and procedures to guide decisions about data exchange and reporting Contracts or MOAs involving data exchange
7.	Has the data governance policy been documented and communicated in an open an accessible way to all stakeholders?	Documented methods of distribution to include who was contacted and how Professional development for all who have access to PII

Laws, Statutory, Regulatory, and Contractural Security Requirements

The District will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. The District's data governance policy and procedures are informed by the following laws, rules, and standards, among others:

A. CIPA: The **Children's Internet Protection Act** was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response. For more information, see: http://www.fcc.gov/guides/childrens-internet-protection-act

B. COPPA: The **Children's Online Privacy Protection Act**, regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information. See www.coppa.org for details.

C. FERPA: The **Family Educational Rights and Privacy Act**, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

D. HIPAA: The **Health Insurance Portability and Accountability Act**, applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well. For more information, see: http://www.hhs.gov/ocr/privacy/hipaa/understanding/
In general, schools are not bound by HIPAA guidelines.

E. PCI DSS: The **Payment Card Industry Data Security Standard** was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. For more information, see www.pcisecuritystandards.org

F. PPRA: The **Protection of Pupil Rights Amendment** affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

These include the right to the following:
Consent before students are required to submit to a survey that concerns one or more of the following protected areas ("protected information survey") if the survey is funded in whole or in part by a program of the U.S.Department of Education (ED)–

1. Political affiliations or beliefs of the student or student's parent;
2. Mental or psychological problems of the student or student's family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating, or demeaning behavior;
5. Critical appraisals of others with whom respondents have close family relationships;
6. Legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
7. Religious practices, affiliations, or beliefs of the student or parents; or
8. Income, other than as required by law to determine program eligibility.

Receive notice and an opportunity to opt a student out of –

1. Any other protected information survey, regardless of funding;
2. Any non-emergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings, or any physical exam or screening permitted or required under State law; and
3. Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others.

For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Data Security Policy

Current Policy 2.36	Adopted: November 3, 2014
The Superintendent is authorized to establish, implement, and maintain data security measures. Procedures to be established include a method of establishing data security classifications, implementing procedural and electronic security controls, and maintaining records regarding security access. The data security measures will apply to Board employees and all Board operations. Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual, may result in appropriate disciplinary action, which may include a recommendation for termination and other legal action.	

Dissemination of Data Governance Policy

The Autauga County Board of Education Data Security Policy is available to the public and all internal stakeholders via the District Policy Manual at www.acboe.net. The detailed policies, provisions, and procedures that serve to implement this policy are outlined in this handbook. Requests for detailed information about the District's data security procedures shall be brought to the committee or the Superintendent who will determine the legitimacy of the request and respond accordingly.

Data Security Measures

I. Purpose

(A) Implement standards and procedures to effectively manage and provide necessary access to System Data, while at the same time ensuring the confidentiality, integrity and availability of the information. Insofar as this policy deals with access to Autauga County Schools' computing and network resources, all relevant provisions in the Data Security Policy are applicable.

(B) Provide a structured and consistent process for employees to obtain necessary data access for conducting Autauga County Schools operations.

(C) Define data classification and related safeguards. Applicable federal and state statutes and regulations that guarantee either protection or accessibility of System records will be used in the classification process.

(D) Provide a list of relevant considerations for System personnel responsible for purchasing or subscribing to software that will utilize and/or expose System Data.

(E) Establish the relevant mechanisms for delegating authority to accommodate this process at the school level while adhering to separation of duties and other best practices.

II. Scope

(A) These Security Measures apply to information found in or converted to a digital format. (The same information may exist in paper format for which the same local policies, state laws, statutes, and federal laws would apply, but no electronic control measures are needed.)

(B) Security Measures apply to all employees, contract workers, volunteers, and visitors of the Autauga County Schools and all data used to conduct operations of the System.

(C) Security Measures do not address public access to data as specified in the Alabama Open Records Act.

(D) Security Measures apply to System Data accessed from any location; internal, external, or remote.

(E) Security Measures apply to the transfer of any System Data outside the System for any purpose.

III. Guiding Principals

(A) Inquiry-type access to official System Data will be as open as possible to individuals who require access in the performance of System operations without violating local Board, legal, Federal, or State restrictions.

(B) The Superintendent and/or his designees shall determine appropriate access permissions based on local policies, applicable laws, best practices, and the Alabama Open Records Act.

(C) Data Users granted "create" and/or "update" privileges are responsible for their actions while using these privileges. That is, all schools or other facilities are responsible for the System Data they create, update, and/or delete.

(D) Any individual granted access to System Data is responsible for the ethical usage of that data. Access will be used only in accordance with the authority delegated to the individual to conduct Autauga County Schools operations.

(E) It is the express responsibility of authorized users to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

(F) These Security Measures apply to System data regardless of location. Users who transfer or transport System data "off-campus" for any reason must ensure that they are able to comply with all data security measures prior to transporting or transferring the data.

IV. Access Coordination

(A) Central Office Department heads, supervisors, area specialists, and principals (Authorized Requestors – those authorized to make requests pertaining to data use/governance) will assist in classifying data sensitivity levels for their areas of expertise

and in identifying which employees require access to which information in order to complete their duties.

(B) The System Technology Coordinator and Technology Supervisor will designate individuals to implement, monitor, and safeguard access to System Data based on the restrictions and permissions determined by the Authorized Requestors using the technical tools available.

(C) Central Office Department heads, supervisors, area specialists, and principals will be responsible for educating all employees under their supervision of their responsibilities associated with System Data security.

Risk Management

A thorough analysis of all the Board of Education's information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats — internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity, which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

The Superintendent or designee will administer periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessments, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

Data Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

A. Personally Identifiable Information (PII)

1. PII is any information about an individual maintained by an agency:

   a. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
   b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

2. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to the District.

B. Confidential Information

1. Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

   a. Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for the District, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

C. Internal Information

1. Internal Information is intended for unrestricted use within the District, and in some cases within affiliated organizations such as the District's business partners. This type of information is already widely-distributed within the District, or it could be so distributed within the organization without advance permission from the information owner.
   a. Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

2. Any information not explicitly classified as PII, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

D. Public Information

1. Public Information has been specifically approved for public release by a designated authority within each entity of the District. Examples of Public Information may include marketing brochures and material posted to the District's web pages.

2. This information may be disclosed outside of the District.

E. Directory Information

The following is the District's list of which student information is to be considered 'directory information':

1. Student first and last name
2. Student gender
3. Student home address
4. Student telephone number
5. Student school
6. Student photograph
7. Student place and date of birth
8. Student dates of attendance (years)
9. Student grade level
10. Student diplomas, honors, awards received
11. Student participation in school activities or school sports
12. Student weight and height for members of school athletic teams
13. Student most recent institution/ school attended
14. Student ID number

Autauga County Schools FERPA Directory Information Disclosure

Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A system administrator may authorize the release of directory information, as defined by Alabama law and the *Family Educational Right to Privacy Act*, for internal administrative purposes or approved educational projects and activities. Public notice of any such release of information shall be given, and parents shall be allowed a reasonable time to object to the release of information.

Compliance

The Data Governance and Use Policy and corresponding handbook applies to all users of the Autauga County School District's information including employees, staff, students, volunteers, and outside affiliates. Failure to comply with such policies and standard by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Autauga County Board of Education procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with the Data Governance and Use Policy by students may constitute grounds for corrective action in accordance with Autauga County Board of Education procedures. Further, penalties associated with state and federal laws may apply.

A. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of PII or Confidential Information as specified in Confidentiality Statement.
2. Unauthorized disclosure of a sign-on code (user id) or password.
3. Attempting to obtain a sign-on code or password that belongs to another person.
4. Using or attempting to use another person's sign-on code or password.
5. Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.
6. Installing or using unlicensed software on the District's computers.
7. The intentional unauthorized destruction of the District's information.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access

Systems and Information Control

All involved systems and information are assets of the District and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

Ownership of Software: All computer software developed by the District's employees or contract personnel on behalf of the District or licensed for the District's use is the property of the District and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

Installed Software: All software packages that reside on computers and networks within the District must comply with applicable licensing agreements and restrictions and must comply with the District acquisition of software policies.

Virus Protection: Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

Access Controls: Physical and electronic access to information systems that contain PII, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the data governance committee and approved by the District. In particular, the data governance committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PII, Confidential and Internal information include (but are not limited to) the following methods:

1. **Authorization:** Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the Data Governance Committee. Any of the following methods are acceptable for providing access under this policy:

   a. Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.

   b. Role-based access: An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

   c. User-based access: A security mechanism used to grant users of a system access based upon the identity of the user.

2. **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PII, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

   a. At least one of the following authentication methods must be implemented:

      1. Strictly controlled passwords

2. Biometric identification, and/or
3. Tokens in conjunction with a PIN.

b. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

c. An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).

d. The user must log off or secure the system when leaving it.

3. **Data Integrity:** The District must be able to provide corroboration that PII, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

   a. transaction audit
   b. disk redundancy (RAID)
   c. ECC (Error Correcting Memory)
   d. checksums (file integrity)
   e. encryption of data in storage
   f. digital signatures

4. **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

   a. integrity controls and
   b. encryption, where deemed appropriate

5. **Remote Access:** Access into the District's network from outside will be granted using the District's approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PII, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the District's network.

6. **Physical Access:** Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals. The following physical controls must be in place:

   a. Computer systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

b. File servers containing PII, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

c. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards.

d. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

1. **Contingency Operations —** Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
2. **Facility Security Plan —** Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
3. **Access Control and Validation —** Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
4. **Maintenance records —** Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

7. **Physical Security** Controls are implemented to protect information system resources, the facility housing those resources, and the facilities used to support their operation. To protect against loss of control over system integrity and system availability, the District will address physical access controls, environmental controls, fire safety, and protect systems and data storage media from theft.

- Ensure computer systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Ensure laptop and portable computers are secured with an appropriate physical security device such as a lockdown cable. Computer equipment installed in public areas shall be similarly secured.
- Control access to areas containing servers, data stores, and communications equipment. Access to secured areas shall be controlled by the use of access card keys, access code keypads, or key locks with limited key distribution. A record shall be maintained of all personnel who have authorized access.

- Closely control keys (where utilized). If a key is reported as missing, change or re-key the corresponding lock(s).
- Maintain a log of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months.
- Ensure visitors are escorted by a person with authorized access to the secured area.
- Ensure each facility containing computer and communications equipment has an appropriate fire suppression system and/or a class C fire extinguisher readily available and in working order.
- Store equipment above the floor, in racks whenever feasible, or on a raised floor to prevent damage from dampness or flooding. Use of water/moisture sensors is recommended.
- Monitor and maintain data center temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
- Store electronic media in secured and environmentally controlled areas, in fire safe containers whenever feasible. Backup/archive media shall, whenever feasible, be stored in a secure off-site storage facility.
- Monitor and control the delivery and removal of all asset-tagged and/or data-storing IT equipment. Maintain a record of all such items entering or exiting their assigned location.
- Ensure that equipment being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

8. **Emergency Access:** Each school is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

   Procedures must be documented to address:

   a. Authorization,
   b. Implementation
   c. Revocation

Equipment and Media Controls*:* The disposal of information must ensure the continued protection of PII, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and

electronic media that contain PII into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

1. Information Disposal / Media Re-Use of:

a. Hard copy (paper and microfilm/fiche)
b. Magnetic media (floppy disks, hard drives, zip disks, etc.) and
c. CD ROM Disks

2. Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore.

3. Data backup and Storage: When needed, create a retrievable, exact copy of electronic PII before movement of equipment.

4. PII and Confidential Information stored on external media (diskettes, cd-roms, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as **PII** or Confidential Information. Further, external media containing PII and Confidential Information must never be left unattended in unsecured areas.

5. PII and Confidential Information must never be stored on mobile computing devices

(laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

a. Power-on passwords
b. Auto logoff or screen saver with password
c. Encryption of stored data or other acceptable safeguards approved by Information Security Officer
d. Mobile computing devices must never be left unattended in unsecured areas.

6. If PII or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of the District. Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with the District.

Data Transfer/Exchange/Printing:

1. Electronic Mass Data Transfers: Downloading, uploading or transferring PII, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, information for research or

any other purposes that include PII must be in accordance with this policy and be approved by the data governance committee. All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Memorandum of Agreements (MOA) must be in place when transferring PII to external entities.

2. **Other Electronic Data Transfers and Printing:** PII, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PII and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible should be de-identified before use.

Oral Communications: All District staff should be aware of their surroundings when discussing PII and Confidential Information. This includes the use of cellular telephones in public areas. All District staff should not discuss PII or Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semiprivate rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

Audit Controls: Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PII must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years.

Evaluation: The District requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

Contingency Plan: Controls must ensure that the District can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PII, Confidential, or Internal Information.

Data Backup Plan: A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.

1. Backup data must be stored in an off-site location and protected from physical damage.
2. Backup data must be afforded the same level of protection as the original data.

3. Disaster Recovery Plan: A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
4. Emergency Mode Operation Plan: A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
5. Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.
6. Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

Data Quality

Supervisory Responsibilities

It is the responsibility of all supervisors to set expectations for data quality and to evaluate their staff's performance relative to these expectations annually. Supervisors should immediately report incidents where data quality does not meet standards to their superior and to any other relevant department, including the State Department of Education, if applicable.

Job Descriptions

Job descriptions for employees whose responsibilities include entering, maintaining or deleting data shall contain provisions addressing the need for accuracy, timeliness, confidentiality and completeness. This includes, but is not limited to: School Registrars, Counselors, Special Education Staff and CNP Staff handling free and reduced lunch data. Teachers shall have the responsibility to enter grades accurately and in a timely manner. School Administrators shall have the responsibility to enter discipline information accurately and in a timely manner.

Transfer of Data to External Service Provider

Personally Identifiable Information (PII) may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes or direct connection to server SQL database for data extraction.

1. No sensitive data, or FERPA protected educational records, will be transferred to an external service provider without prior approval of the Data Governance committee. Exception: Alabama State Department of Education.

2. No school or department should enter into a contract for the use of any program that requires the import of District data without first consulting and receiving approval from the Data Governance committee.

3. The Data Governance committee will determine which of the following should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer:

   a. Contract
   b. Designating the service provider as an "Official" as defined in FERPA
   c. Memorandum of Understanding
   d. Memorandum of Agreement
   e. Non-Disclosure Agreement

4. Non-Disclosure Agreement (NDA) Information and Sample NDA

The following instructions comply with Autauga County Schools Policy Data Security

When to Use a Non-Disclosure Agreement

1. Private Information. Confidential information, as defined by FERPA and other regulations and policies, is to be protected and disclosed only to those employees who have a direct legitimate reason for access to the data in order to provide educational services to the student.

2. You must seek guidance from the Pupil Services, Special Education, and/or the Technology Department prior to transferring confidential information to any outside company, online service (free websites), or to any outside individual, organization, or agency without the explicit written permission of the parent of a minor student or an adult-aged student. This information includes:

   1) Social Security number
   2) Grades and test scores (local and standardized)
   3) Special education information
   4) Health information and 504 information
   5) Attendance information (not enrollment, but specific attendance dates)
   6) Family/homeless/or other similar status
   7) Child Nutrition Program status (free or reduced meals)

   This includes providing confidential information to individuals, including System employees, for use in dissertations or other studies for college courses or doctorial studies. Refer all such requests, including those for federal, state, or other studies to the appropriate Central Office personnel for their approval before releasing any such individualized information. Approved recipients may be required to complete an NDA so that they fully understand their responsibilities with regard to safeguarding and later destroying this private information. This restriction does not apply to publicly available aggregated data such as dropout rates, attendance rates, percentage of free and reduced lunch program students.

   Exceptions. Other Public K-12 Schools - Private information may be transferred upon request to the State Department of Education or other school systems with a legitimate need for the data;

however, the transfer process should comply with data security protocols (see below). In addition, personnel must research all recipients to ensure that the school is a legitimate school.

Colleges – Confidential information may be transferred to institutions of higher education, when the adult student or the parent of a minor student requests that transcripts or other private information be released to specific institutions. Such information should not be transferred to colleges based on a request from the college directly, unless approved by the individual whose records will be transferred.

3. Directory Information. Although Autauga County Schools has identified the following as "Directory Information," schools should still carefully consider the transfer or publication of this information. Seek guidance when in doubt. Much of this information, combined with data collected elsewhere can be used for identity theft purposes, stalking, and other unlawful or unethical purposes.

    1) Home address
    2) Home or cell phone numbers of students or their parents
    3) Email addresses of students or their parents
    4) Date and place of birth

    Exception: U.S. Military and institutions of higher learning for recruiting purposes. However, schools must first determine which parents have submitted Opt Out forms relative to these requests prior to transferring data.

Nondisclosure Agreement

THIS NONDISCLOSURE AGREEMENT (this "Agreement"), by and between AUTAUGA COUNTY SCHOOLS, AL (the "District"), and _____ (the "Service Provider"), relates to the disclosure of valuable confidential information. The "District" refers to all schools, departments, and other entities within Autauga County Schools. The Service Provider refers to any free or fee-based company, organization, agency, or individual which is providing services to the District or is conducting District-approved academic research. The Disclosing Party and the Receiving Party are sometimes referred to herein, individually as a "Party" and collectively, as the "Parties."

To further the goals of this Agreement, the Parties may disclose to each other, information that the Disclosing Party considers proprietary or confidential.

The disclosure of District's Confidential Information by a Receiving Party may result in loss or damage to the District, its students, parents, employees, or other persons or operations. Accordingly, the Parties agree as follows:

Confidential Information disclosed under this Agreement by the District shall only be transmitted in compliance with the District's approved security protocols. The Receiving Party must accept the data transmitted in these formats.

The Service Provider will request or receive Confidential Information from the District solely for the purpose of entering into or fulfilling its contractual obligations or pre-approved academic research.

The Service Provider agrees not to use, or assist anyone else to use, any portion or aspect of such Confidential Information for any other purpose, without the District's prior written consent.

The Service Provider will carefully safeguard the District's Confidential Information and may be required to describe such safety measures to the District upon request.

The Service Provider will not disclose any aspect or portion of such Confidential Information to any third party, without the District's prior written consent.

Confidential Information disclosed under this Agreement shall not be installed, accessed or used on any computer, network, server or other electronic medium that is not the property of the District or the Service Provider, or to which third-parties have access, unless otherwise provided in a separate contract or agreement between the Parties hereto.

The Service Provider shall inform the District promptly if the Service Provider discovers that an employee, consultant, representative or other party, or any outside party has made, or is making or threatening to make, unauthorized use of Confidential Information.

The Service Provider shall immediately cease all use of any Confidential Information and return all media and documents containing or incorporating any such Confidential Information within five *(5)* days to the District after receiving written notice to do so, or whenever the contract for services between the District and the Service Provider expires or is terminated. In addition, the Service Provider may be required by the District to destroy any Confidential Information contained on primary or backup media upon written request of the District.

Date	Date
District	Service Provider
Printed Name	Printed Name
Signature	Signature
Title	Title
Phone/Email	Phone/Email

Confidential Information includes:

- any written, electronic or tangible information provided by a Disclosing Party
- any information disclosed orally by a Disclosing Party that is treated as confidential when disclosed
- all information covered by FERPA or other local, state, or federal regulation applying to educational agencies
- any other information not covered by FERPA, HIPAA, or other local, state, or federal regulation which the District requires the Service Provider to treat as confidential

Reporting Security Breaches

All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical security measures.

Data Governance Training

I. School and Central Office Administrators

(A) School and Central Office Administrators will receive refresher training on FERPA and other data security procedures annually

(B) Principals and Central Office Administrators shall contact the Technology Coordinator or the Data Manager when in doubt about how to handle data.

(C) Principals and Central Office Administrators will be kept aware of emerging issues pertaining to data security.

II. School Support Staff

(A) School support staff will be trained and refreshed on FERPA and other data security procedures annually.

(B) School support staff's adherence to the data security procedures may be monitored by the appropriate Central Office personnel through random audits.

III. Teacher and Staff Training

(A) All teachers will complete training on all District technology policies, including how their use of technology is governed by FERPA and other data security procedures established by the District.

(B) All department heads will be expected to educate their support staff on data governance as it applies to their department's work.

(C) All users will receive reminders throughout the year via email regarding issues such as malware threats and phishing scams and how to report suspected threats.

IV. Parent / Volunteer Training

(A) School administrators and designees shall educate parent/volunteer groups about FERPA and student confidentiality. For instance, organizations who intend to post information about the school's students or activities should not compromise the privacy of students in protective custody. Because the school cannot tell these groups which students may be in

such situations, the organization should be cautioned about exposing any information or photos that could cause harm to students or their families.

(B) School officials will have procedures that include educational materials for school-related organizations who wish to post their own websites.

InformationNOW Access

InformationNOW (Now) enables authorized users to access the application from anywhere they may have Internet access. In response to this anywhere/anytime access, the Data Governance Committee has implemented the following:

1. **Strong password requirement for iNow logins** - Users are responsible for complying with the following password standards:
   - Passwords should never be shared with another person
   - Password should be changed on a regular basis
   - Passwords must have a minimum length of (six) characters and (one) Number.
   - Passwords should never be saved when prompted by any application or browser.
   - Passwords should not be programmed into a PC or recorded anywhere that someone may find and use them.
   - When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc...). A combination of alpha and numeric characters are more difficult to guess.

2. **Data Security Guidelines**
   Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data. All employees that have access to Autauga County Schools' student and employee data have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner. Access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

   - Transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.
   - Copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD. In addition, student and employee data should never be removed from the school premises on a laptop or other mobile device.

- Employees should keep their computer workstation secure by locking or logging off when the machine is unattended.
- Employees should never share network or program passwords with others.
- Employees should not allow personal data that has been printed into the view or hands of unintended parties.
- Employees should not use their software rights to grant others permission to data to which they are not entitled.

Notice of Risks Related to INOW Usage

INOW Access for Parent Volunteers

Some schools rely on parent volunteers to help greet visitors and locate students. Due to FERPA and other confidentiality expectations volunteers should only be granted very limited INOW rights. In most cases this should be the 'Student Schedule Locator' level of access which enables the volunteer to see a list of all students and their schedules. Remember, INOW permissions are web-based so what volunteers can see from the school, they can also access from anywhere they have Internet access.

Concerns about Parent Volunteers Checking Students Out of School

Releasing a child from school into the care of someone else is a serious responsibility. Schools should carefully assess whether or not the "check-out" information is always up to date. In the past school personnel have raised concerns that parents often change their minds about who can and cannot check out their children, but they don't necessarily notify the school in a timely manner. This makes the prospect of allowing parent volunteers who are unfamiliar with the current circumstances of various family situations to check out students an area of concern.

Allowing Others to Use Another User's INOW Account to 'Give' them Greater Access is Prohibited

A user's INOW permission level is based on their job responsibilities. Violating FERPA can have serious consequences, including the loss of Federal Funding and other legal liabilities. Since we have a responsibility to protect our student and employee data from identity theft or other misuse, no one may log into INOW and allow others to use their access. Participating in this practice violates our Acceptable Use policies and Data Security Procedures.

Plan for when School Personnel is Out for an Extended Period

You should have a plan for occasions when your secretary/registrar is out sick or on extended leave. Anyone filling in for the secretary/registrar should be a bona fide employee, not a volunteer.

Providing Information to Others on Students NOT Enrolled at Your School

INOW rights intentionally prevent the staff at one school from seeing information on students at another school, which complies with FERPA guidelines. The only exception is for district level personnel who have specific needs to see all school data and teachers or others who serve specific students in multiple schools.

It is important that staff members at one school do not attempt to give information about students enrolled in another school to individuals who ask for such information. Instead they should expect the person asking for the information to contact that school themselves.

DO NOT tell an individual who has no official right to know where else the student is enrolled. Even if the person asking is a parent, there may be a dangerous situation that you are now unaware of, so the safe action to take is to refer such requests to the Pupil Services Department. The danger in telling someone, employee or not, what other school the child is enrolled in lies in the fact that you have no access to that student's record and will not know if the child is in protective custody or is involved in some other situation such as custody dispute, etc. This could result in a safety issue. This rule applies even when the person asking for the information is one of our own employees..

Autauga County Schools Data Security Agreement

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Autauga County Schools' student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.

I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

I understand that transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.

Except when explicitly instructed to do so by school or district administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive, CD, or other electronic device, such as laptos, tablets, or ipads..

I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled.

Please sign below to indicate you understand and agree to the above statements.

Printed Name	Signature
Date	Location